



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER LAW IN INDIA: EMERGING ISSUES AND CHALLENGES

Srabanti Biswas

ABSTRACT

The rapid expansion of digital technology has changed the way people communicate, work, make payments and access public services in India. At the same time, it has created new opportunities for cybercrime and raised complex legal and security concerns. This paper examines the development of cyber law in India and the major issues and challenges emerging from the increasing use of digital technologies. It focuses on the Information Technology Act, 2000, the IT Amendment Act, 2008, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nyaya Sanhita, 2023, along with the role of institutions such as CERT-In, NCIIPC and I4C. The paper also discusses emerging concerns including artificial intelligence, deepfakes, ransomware, cryptocurrency, data breaches, privacy, digital evidence and cross-border cybercrime. It highlights the important role of the judiciary in balancing technological development with fundamental rights. The study argues that keeping pace with cybercrime requires not only updated laws but also effective enforcement, stronger cybersecurity measures, international cooperation and greater public awareness. A balanced approach is therefore necessary to ensure that India's digital growth remains secure, accountable and respectful of individual rights.

Keywords: Cyber Law; Cybercrime; Cybersecurity; Data Privacy; Digital Evidence.

I. INTRODUCTION

The rapid development of information and communication technology has fundamentally changed the way people communicate, conduct business, make payments, access public services and store information. During the 1990s and early 2000s, the increasing use of computers and the internet created new forms of criminal activity that traditional laws were not

specifically designed to address. As economic and governmental activities gradually moved from paper-based systems to digital platforms, the need for a dedicated legal framework became increasingly important. India responded to this development through the Information Technology Act, 2000, which provided legal recognition to electronic records and electronic transactions while also creating provisions to deal with several computer-related offences¹.

India's digital transformation has produced major advantages in areas such as public administration, banking, education, healthcare and commerce. Digital India, Aadhaar, DigiLocker, online government services, UPI and social-media platforms have made services faster and more accessible. At the same time, the greater dependence on digital infrastructure has created a larger environment for cybercriminals to exploit. Personal information, financial credentials and government databases can become targets for theft, manipulation or unauthorized access. Consequently, cybersecurity is no longer merely a technical issue; it has become a legal, economic, social and constitutional concern².

The Information Technology Act, 2000 marked the beginning of India's dedicated cyber-law framework. Its original purpose was closely connected with the legal recognition of electronic records, electronic communication and electronic transactions. As technology developed and cybercrime became more complex, the original framework required substantial modification. The Information Technology (Amendment) Act, 2008 expanded the legislation by introducing or strengthening provisions relating to identity theft, online cheating, cyber terrorism, data protection, intermediary responsibility and other forms of cyber misconduct. This demonstrated that cyber law must continuously adapt because technological development often creates risks that were not anticipated when earlier legislation was drafted.

II. EVOLUTION IN INDIA

Cybersecurity involves the legal, technical and organizational measures used to protect digital systems, networks and data from unauthorized access, misuse and disruption. India's rapid digitalisation through Digital India, UPI, cloud computing, e-commerce, digital banking and Aadhaar-based services has significantly increased its digital dependency and attack surface. Threats such as ransomware, phishing, identity theft, financial fraud, data breaches and cyber espionage have consequently become major concerns. Incidents such as the 2022 AIIMS

¹ Vanshika Sharma, *Cyber Law in India: Emerging Issues and Challenges*, 3 IJRLM, (last visited on Sep. 25, 2026, 10.00 P.M.), <https://ijrlm.com/wp-content/uploads/jms/ms/6a806f163b6cd.pdf>.

² Hitesh Lathar, *Cybercrime and Data Protection Laws in India: Emerging Legal Challenges*, 3 IJARMT 668, 668 (2026).

ransomware attack demonstrate the potential impact of cyberattacks on essential public services. Cybersecurity has therefore become an important issue of national security, economic stability and individual privacy.

Since the 1990s, the increasing use of technology in communication, commerce, banking and governance created a need for laws specifically addressing electronic transactions and cybercrime. Traditional laws were inadequate for dealing with emerging digital offences, making the development of dedicated cyber legislation necessary³.

The development of cyber law in India has followed the expansion of digital technology. The Information Technology Act 2000 provided the initial legal foundation by recognizing electronic records and digital signatures and addressing computer-related offences. The Information Technology (Amendment) Act 2008 subsequently expanded the framework to include identity theft, online impersonation, cyber terrorism, data protection and intermediary responsibilities. More recently, the Digital Personal Data Protection Act 2023 introduced a dedicated framework for regulating digital personal data, while CERT-In directions and sector-specific regulations have strengthened cybersecurity obligations. This evolution reflects India's transition from regulating electronic transactions to addressing broader concerns of privacy, cybersecurity and digital governance⁴.

III. CONSTITUTIONAL FRAMEWORK

Although the Constitution does not expressly refer to cyberspace, fundamental rights apply to the digital environment. Freedom of speech and expression under Article 19(1)(a) extends to online communication, subject to reasonable restrictions under Article 19(2). The Supreme Court's decision in *Justice KS Puttaswamy (Retd) v Union of India* recognized privacy as a constitutionally protected right under Article 21. Consequently, cyber regulation must balance security and crime prevention with privacy, freedom of expression and other fundamental rights.

IV. STATUTES

INFORMATION TECHNOLOGY ACT 2000

The IT Act 2000 remains a key component of India's cyber law framework. Initially enacted

³ Vanshika Sharma, *Cyber Law in India: Emerging Issues and Challenges* 3 IJRLM, 2026 (last visited on Sep. 25, 11.45 P.M.) <https://ijrlm.com/wp-content/uploads/jms/ms/6a806f163b6cd.pdf>.

⁴ Ankita Shrivastava and Sapna et. al., Legal Challenges of Cybersecurity in Indian and International Scenarios 13 TIJER b95, b95-96 (2026).

to facilitate electronic commerce and recognize electronic records and signatures, its scope subsequently expanded to address various forms of cybercrime and digital misconduct. The principal objectives of the IT Act include recognizing electronic records and signatures, facilitating e-governance, regulating Certifying Authorities, preventing cyber offences and protecting computer systems and electronic data.

IMPORTANT PROVISIONS OF THE INFORMATION TECHNOLOGY ACT

1. SECTION 43 – Section 43 provides civil liability for specified unauthorized acts involving computer systems, including unauthorized access, copying or extraction of data, introduction of harmful programs and damage or disruption to computer resources.

2. SECTION 43A – Section 43A imposes liability on covered organizations for negligent failure to maintain reasonable security practices in protecting sensitive personal data, subject to the statutory framework.

3. SECTION 65 – Section 65 criminalizes intentional concealment, destruction or alteration of computer source code where the law requires the source code to be maintained.

4. SECTION 66 – Section 66 makes certain acts covered by Section 43 criminal when they are committed dishonestly or fraudulently. It therefore distinguishes specified criminal conduct from conduct attracting civil liability.

5. SECTION 66C – Section 66C criminalizes dishonest or fraudulent use of another person's electronic signature, password or other unique identification features. It is particularly relevant to online identity theft and unauthorized access to digital accounts.

6. SECTION 66D – Section 66D addresses cheating by personation carried out through communication devices or computer resources, covering various forms of digital impersonation and online fraud.

7. SECTION 66E – Section 66E addresses the intentional capture, publication or transmission of images of a person's private areas without consent in circumstances covered by the provision. It provides specific statutory protection against certain forms of digital privacy violation.

8. SECTION 66F – Section 66F deals with cyber terrorism involving conduct intended to threaten India's sovereignty, integrity, security or critical information infrastructure and provides severe criminal penalties for conduct meeting its statutory requirements.

9. SECTION 67 –Section 67 criminalizes the publication or transmission of obscene material in electronic form, subject to the requirements of the provision.

10. SECTION 69 – Section 69 empowers the Central Government, subject to statutory conditions and procedures, to direct interception, monitoring or decryption of information in specified circumstances relating to matters such as national security, defence, public order and prevention or investigation of offences.

11. SECTION 72 – Section 72 provides consequences for unauthorized disclosure of information obtained through powers conferred under the IT Act, thereby protecting confidentiality and privacy in specified circumstances.

12. SECTION 79 – Section 79 provides conditional safe-harbour protection to intermediaries for third-party information, subject to compliance with applicable statutory duties and due-diligence requirements. This provision is particularly significant for social media platforms, online marketplaces and other digital intermediaries⁵.

DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 establishes a statutory framework for processing digital personal data. It places obligations on Data Fiduciaries and provides certain rights to Data Principals, while also addressing children's data, grievance redressal and penalties for specified violations. The principal challenge is ensuring effective implementation while balancing privacy, innovation, commercial interests and legitimate governmental requirements.

BHARATIYA NYAYA SANHITA 2023

The Bharatiya Nyaya Sanhita 2023 operates alongside the Information Technology Act where traditional criminal conduct is carried out through digital technologies. Cyber-enabled cheating, forgery, stalking, intimidation and financial offences may therefore involve both general criminal law and specialized cyber provisions. This overlap can create challenges concerning classification of offences, investigation, jurisdiction and coordination between investigating authorities⁶.

⁵ Vanshika Sharma, *Cyber Law in India: Emerging Issues and Challenges*, 3 IJRLM, 2026 (last visited on Sep. 26 2026, 10.00 P.M.) <https://ijrlm.com/wp-content/uploads/jms/ms/6a806f163b6cd.pdf>.

⁶ Yashi Agarwal, *Cyber Law in India: Emerging Issues and Challenges*, 3 IJRLM, (last visited on Sep. 26, 2026, 12.45 P.M.) <https://ijrlm.com/wp-content/uploads/jms/ms/6a4137799ad65.pdf>.

INSTITUTIONAL MECHANISMS: CERT-IN, NCIIPC AND I4C AND INTERNATIONAL LEGAL OVERVIEW

- India has created several institutions to manage cybersecurity and cybercrime. CERT-In, under Section 70B of the IT Act, responds to cyber incidents, issues security alerts, and coordinates with national and international agencies. Its 2022 directions require organizations to report serious cyber incidents within six hours and retain logs for 180 days. NCIIPC, established under Section 70A, protects critical sectors such as banking, energy, telecom, transport, and government systems. I4C, under the Ministry of Home Affairs, coordinates cybercrime investigations, manages the National Cyber Crime Reporting Portal, and operates the 1930 helpline for financial fraud. Indian courts have significantly shaped cyber law through important judgments. Shreya Singhal (2015) protected online freedom of speech by striking down Section 66A and clarified intermediary liability. Puttaswamy (2017) recognised privacy as a fundamental right and strengthened the basis for personal data protection. Anvar P.V. (2014) established requirements for admitting electronic evidence, while Suhas Katti (2004) became an early precedent for addressing online harassment.
- The Budapest Convention (2001) provides an international framework for combating cybercrime and collecting digital evidence. Its 2022 additional protocol strengthened cross-border access to electronic evidence. India has not ratified the Convention, although parts of the IT Act are broadly aligned with it. The GDPR gives individuals stronger control over their personal data through rights such as access, correction, deletion, and portability. Its wide territorial reach and strict penalties have influenced data protection laws in several countries, including India.
- The UN-GGE and OEWG have developed principles for responsible state behaviour online, including protection of critical infrastructure and application of international law to cyberspace. The UN Cybercrime Convention adopted in 2024 is another major step toward international cooperation, although concerns remain about privacy and surveillance. Cyber warfare can disrupt infrastructure, governments, and economies, as shown by major incidents such as Stuxnet and NotPetya. Although principles of international humanitarian law can apply to cyber operations, their practical use remains debated. The Tallinn Manual 2.0 provides legal guidance, while India's Defence Cyber Agency supports military cyber capabilities. However, a clear statutory framework for military cyber operations is still needed. Global cyber laws remain difficult to harmonise because countries follow different rules on privacy, data

localisation, government access, and state cyber operations. Cross-border investigations are further complicated by differences in jurisdiction, evidence rules, and technical capacity. These gaps can allow cybercriminals to operate from countries with weaker enforcement⁷.

V. EMERGING ISSUES AND CHALLENGES IN CYBER LAW

Rapid technological development has made cybercrime more complex, involving AI, ransomware, cryptocurrency, deepfakes, cloud computing, and cross-border offences. India has strengthened its cyber laws, but gaps still remain in effectively regulating new digital risks while protecting individual rights.

- i. **ARTIFICIAL INTELLIGENCE AND DEEPFAKE TECHNOLOGY-** AI is transforming many areas of life, but it is also creating new cyber risks. AI can generate convincing fake messages, adaptive malware, and manipulated identities, making traditional security measures less effective and creating challenges for existing laws.
- ii. **DEEPFAKE TECHNOLOGY-** Deepfakes use AI to create realistic fake images, videos, and audio that can be used for impersonation, misinformation, fraud, and privacy violations. India currently relies on existing IT, criminal, copyright, and privacy laws, showing the need for a clearer and comprehensive legal framework for AI-generated content.
- iii. **DATA PRIVACY AND PERSONAL DATA PROTECTION-** Digital platforms collect large amounts of sensitive personal information, increasing the risks of identity theft, fraud, surveillance, and privacy breaches. The **Puttaswamy judgment** recognised privacy as a fundamental right, while the **DPDP Act, 2023** introduced rules for consent, accountability, and individual control over personal data. However, cross-border data transfers, surveillance, algorithms, and enforcement remain challenging.
- iv. **CRYPTOCURRENCY AND FINANCIAL CYBERCRIME-** Cryptocurrency has created new opportunities for digital finance but can also facilitate ransomware, fraud, illegal transactions, and other financial crimes. Although India taxes virtual digital assets and applies anti-money-laundering rules, a comprehensive cryptocurrency law is still lacking.
- v. **RANSOMWARE ATTACKS-** Ransomware can lock important data and disrupt essential services such as hospitals, schools, finance, transport, and government

⁷ Ankita Shrivastava and Sapna *et. al.*, *Legal Challenges of Cybersecurity in Indian and International Scenarios*, 13 TIJER b95, b99-b102 (2026).

systems. As attacks become more advanced, stronger security measures, faster response systems, international warnings, and cooperation are necessary.

- vi. **CYBER TERRORISM AND NATIONAL SECURITY-** Cyber terrorism can target critical infrastructure and essential services, creating serious national security risks. Since attackers can hide their identities and operate through multiple systems, investigation is difficult. Section 66F of the IT Act addresses cyber terrorism, while stronger cyber defences and international cooperation are needed.
- vii. **DARK WEB AND ORGANISED CYBERCRIME-** The Dark Web provides anonymity that can be used for both privacy and criminal activities. Organised criminals may trade illegal goods, stolen data, malware, and other prohibited material, while encryption and cross-border operations make investigation difficult.
- viii. **JURISDICTIONAL CHALLENGES-** Cybercrime can involve several countries at the same time, creating uncertainty over jurisdiction, applicable laws, evidence collection, and prosecution. Differences between legal systems and slow international cooperation make cross-border cybercrime investigations more difficult⁸.
- ix. **DIGITAL EVIDENCE AND FORENSIC CHALLENGES-** Digital evidence from emails, phones, servers, CCTV, blockchain, and cloud platforms is increasingly important in cybercrime cases. Since such data can be changed, deleted, or encrypted, skilled forensic investigation and proper chain-of-custody procedures are essential.
- x. **CYBER THREATS-** Cyber threats are malicious activities designed to damage systems, disrupt networks, or misuse digital devices. Common examples include Trojan attacks, advanced persistent threats, and phishing through fake emails or messages.
- xi. **DIGITAL CONTENT OFFENCES, CYBERBULLYING AND HARASSMENT-** Online content offences include identity theft, cyberbullying, phishing, cyberstalking, morphing, hate speech, and child sexual abuse material. Indian cyber and criminal laws provide provisions for dealing with several of these offences.
- xii. **FRAUDULENT ACTIVITIES IN CYBERSPACE-** Cyber fraud involves deceiving people or organisations to obtain money, personal information, or electronic credentials. Common examples include credit-card and OTP scams, identity theft, investment fraud, and Aadhaar-related fraud⁹.

⁸ Vanshika Sharma, *Cyber Law in India: Emerging Issues and Challenges* 3 IJRLM, 2026 (last visited on Sep. 26 2026, 10.00 P.M.) <https://ijrlm.com/wp-content/uploads/jms/ms/6a806f163b6cd.pdf>.

⁹ Cyber Law in India: Guardian of the Digital Realm, Indian Legal Blog, LexisNexis (last visited on Sep. 27, 2026, 2.00 P.M.) <https://www.lexisnexis.com/blogs/in-legal/b/law/posts/cyber-law-in-india-guardian-of-the-digital-realm>.

V. KEY INCIDENTS AND STATISTICS

- a. India witnessed a sharp increase in cybersecurity incidents, rising from 10.29 lakh in 2022 to 22.68 lakh in 2024, showing the growing scale of cyber threats.
- b. By 28 February 2025, cyber fraud reported through the NCRP had resulted in significant financial losses, highlighting the increasing impact of online fraud.
- c. Emerging fraud methods such as spoofing, AI-generated deepfakes and phishing are increasingly being used to deceive victims and obtain sensitive information.
- d. Fraudsters are increasingly targeting UPI transactions, including through compromised mobile numbers, demonstrating vulnerabilities in digital payment systems.
- e. Fraudulent online betting platforms have reportedly generated over ₹400 crore in criminal proceeds, often by attracting users with promises of high returns.
- f. Authorities have blocked over 9.42 lakh SIM cards and 2,63,348 IMEIs associated with fraudulent activities as part of efforts to disrupt cybercrime networks.
- g. By March 2025, CERT-In had conducted 109 cybersecurity mock drills involving 1,438 organizations to test and improve their cyber preparedness.
- h. The I4C has blocked 3,962 Skype IDs and 83,668 WhatsApp accounts reportedly linked to cyber fraud.
- i. The CFCFRMS has helped prevent losses of more than ₹5,489 crore across over 17.82 lakh reported cyber-fraud complaints.
- j. The Samanvaya Platform has supported cybercrime investigations by contributing to 12,987 arrests, 1,51,984 criminal linkages and 70,584 investigation-assistance requests¹⁰.

VI. JUDICIAL DECISIONS

Shreya Singhal v. Union of India¹¹- In Shreya Singhal (2015), the Supreme Court struck down Section 66A of the IT Act for violating freedom of speech. The decision highlighted the danger of vague legal provisions that could restrict legitimate online expression.

¹⁰ Press Information Bureau, Government of India, Curbing Cyber Frauds in Digital India, 2025 (last visited on Sep. 27, 2026, 11.49 P.M.) <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/oct/doc2025108660701.pdf>.

¹¹ Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Justice K.S. Puttaswamy v. Union of India¹²- In Puttaswamy (2017), a nine-judge Supreme Court bench recognised privacy as a fundamental right under Article 21. The judgment provided an important constitutional basis for protecting personal and informational privacy.

Anvar P.V. v. P.K. Basheer- Anvar P.V. (2014)¹³ clarified that electronic records must satisfy the requirements of Section 65B for admission as evidence, strengthening the procedural standards for digital evidence.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal¹⁴- Arjun Panditrao Khotkar (2020) reaffirmed the importance of Section 65B certification for electronic evidence and clarified the law relating to its admissibility in court.

Avnish Bajaj v. State (NCT of Delhi)¹⁵- The Avnish Bajaj/Bazee.com case addressed the responsibility of online intermediaries for unlawful content and contributed to the development of intermediary liability and safe-harbour principles under Section 79 of the IT Act¹⁶.

VII. ADDRESSING THE CHALLENGES FACED BY CYBER LAWS IN INDIA

Cybercrime is constantly changing, so India's cyber laws also need to keep developing. This requires a combined effort through updated laws, better-trained authorities, international cooperation, stronger cybersecurity systems, public awareness, easier reporting, a well-equipped judiciary, and cooperation between the government and private sector.

1. LEGISLATIVE REFORMS- Technology changes very quickly, and criminals often find new ways to misuse it. Therefore, cyber laws should be regularly reviewed and updated. Lawmakers should also work with cybersecurity experts, technology companies and civil society to identify gaps and make the law more effective.

2. INTERNATIONAL COOPERATION- Cybercrime does not stop at national borders. A criminal may be in one country, use a server in another and target a victim somewhere else. For this reason, India needs stronger international cooperation, information sharing and joint efforts to investigate and tackle cybercrime.

3. CAPACITY BUILDING- Having good laws is not enough if investigators do not have the skills and technology needed to enforce them. Police and other enforcement agencies should

¹² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹³ Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

¹⁴ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

¹⁵ Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769 (Del).

¹⁶ Vanshika Sharma, Cyber Law in India: Emerging Issues and Challenges, 3 IJRLM, 2026(last visited on Sep. 27, 2026, 10.00 P.M), <https://ijrlm.com/wp-content/uploads/jms/ms/6a806f163b6cd.pdf>.

receive regular training in cyber investigations, digital forensics and technology, along with access to modern investigative tools.

4. PUBLIC AWARENESS AND EDUCATION- Many cybercrimes can be prevented when people know how to stay safe online. Therefore, awareness programmes should educate citizens, businesses and government employees about strong passwords, phishing, online scams, data protection and other basic cyber-safety practices.

5. STRENGTHENING CYBERSECURITY INFRASTRUCTURE- India also needs stronger technical systems to prevent and respond to cyberattacks. This means investing in modern cybersecurity technology, quick incident-response mechanisms and better security practices. Government and private organizations should work together to develop security measures suited to the needs of different sectors.

6. BETTER CYBERCRIME REPORTING- Victims should be able to report cybercrime quickly and easily. Online reporting portals, helplines and support services can help victims get immediate assistance and give law-enforcement agencies a better chance of investigating the crime and recovering losses.

7. STRENGTHENING JUDICIAL CAPACITY- Cybercrime cases often involve complicated technology and digital evidence. Judges and lawyers therefore need a proper understanding of cyber law and digital forensics. Specialized training and, where appropriate, specialized courts can help ensure that such cases are dealt with more efficiently.

8. PUBLIC-PRIVATE PARTNERSHIP- Cybersecurity cannot be handled by the government alone. Technology companies, businesses, universities and civil society also have an important role to play. Working together can improve information sharing, research, technical resources and the overall ability to respond to cyber threats.

9. DEVELOPMENT OF CYBER LAWS IN INDIA- The growth of technology created the need for new legal rules and new categories of offences. Cyber laws should protect users, support law-enforcement agencies and discourage offenders. Technology itself does not commit a crime; it is people who misuse technology to steal, manipulate or destroy information.

10. ROLE OF UNCITRAL- The need for legal recognition of electronic transactions was also recognized internationally. In 1996, UNCITRAL adopted the Model Law on Electronic Commerce, encouraging countries to develop laws that could deal with electronic records and digital transactions.

11. INFORMATION TECHNOLOGY ACT, 2000- Following these developments, India introduced the Information Technology Act, 2000, which became the main legal framework for dealing with electronic records, digital transactions and cyber offences. It also worked alongside existing criminal-law provisions dealing with offences such as forgery, fraud and manipulation of records.

12. RECOGNITION OF ELECTRONIC EVIDENCE- One of the important changes brought by the IT Act was the legal recognition of electronic records and documents. This became increasingly important as communication, transactions and evidence moved from physical to digital formats.

13. MAIN AREAS COVERED BY THE IT ACT- The IT Act provides a legal framework for electronic records, digital signatures, cyber offences and contraventions, and establishes mechanisms for dealing with violations occurring in the digital environment¹⁷.

VIII. CONCLUSION

India's rapid digital growth has brought enormous benefits but has also increased the risk of cybercrime, including financial fraud, ransomware, identity theft, deepfakes and data breaches. The Information Technology Act, 2000, supported by newer laws such as the DPDP Act, 2023, and institutions like CERT-In, NCIIPC and I4C, has strengthened India's response to these challenges.

However, technology is evolving faster than the law. Issues such as AI, privacy, digital evidence, encryption and cross-border cybercrime require continuous legal and institutional reform. Therefore, India needs not only stronger laws but also effective enforcement, international cooperation, better cybersecurity infrastructure and greater public awareness. The ultimate goal should be to ensure that India's digital progress remains secure, accountable and respectful of individual rights.

¹⁷ Kritika Kushwaha, *Cyber Laws in India: Issues and Challenges*, 5 IJLR 361, 363-364 (2025).